



15370 Barranca Parkway
Irvine, CA 92618-2215
USA

iCLASS Hi-O

APPLICATION NOTE

© 2010 HID Global Corporation. All rights reserved.

February 2010

Document Number AN0133, A.0

HID GLOBAL, HID, the HID logo, and iCLASS are the trademarks or registered trademarks of HID Global Corporation, or its licensors, in the U.S. and other countries.

Contents

Contents	1
Overview	2
1 Hi-O Signaling Interface	3
2 Device Identification	7
Contact	8



List of Tables

Table 1 – Virtual Devices.....	3
Table 2 – MIFARE UID Example Data	4
Table 3 – MIFARE UID Hi-O Messaging Sequence.....	4
Table 4 – iCLASS 26 Bit Credential Example Data.....	5
Table 5 – iCLASS 26 Bit Credential Hi-O Messaging Sequence	5
Table 6 – iCLASS Hi-O Reader Light Types	5
Table 7 – ASCII Table for Keypad Characters	6
Table 8 – Keypad Event Hi-O Messaging Sequence	6
Table 9 – Offline States	7
Table 11 – Device Identification Values	7

Overview

The Hi-O[®] system provides for easy component connection at a door. The result is simpler installation and maintenance of a door, while giving increased security through encryption of the controller to reader communications.

The physical layer of the network uses a two-wire Controller Area Network (CAN). CAN was originally developed for communications between automotive electronics, and is a very reliable, low cost solution for networking a small number of devices. The Hi-O[®] implementation consists of two-wires connected to all components around a door plus power and ground.

The upper level communication protocol used by the Hi-O network is based on an open standard called CANopen. CANopen handles the automatic configuration and communication of pre-defined nodes on the network.

In a Hi-O Door, card information, reader control, and door lock control signals are conveyed through a set of messages called Virtual Devices. The set of virtual devices available to a Hi-O network is published in the CAN In Automation Draft Proposal DSP-416 – Application Profile for Building and Door Control.

For more information about Hi-O visit <http://www.hi-o.se>.

1 Hi-O Signaling Interface

1.1 Virtual Devices

The iCLASS® Universal Hi-O reader is intended for use only with a Hi-O capable door controller such as the HID® Edge® Reader. Following is a list of Virtual Devices implemented in the iCLASS Hi-O reader.

Table 1 – Virtual Devices

Virtual Devices	Dir	Description
Identification Event	TX	Conveys access control information obtained from a credential to the door controller.
Keypad Event*	TX	Conveys keypad activation information from an iCLASS Hi-O reader to a door controller.
Device Light Control	RX	Used by the door controller for controlling the LED's on an iCLASS Hi-O Reader.
Device Light Control	RX	Used by the door controller for controlling the beeper on an iCLASS Hi-O Reader
Sabotage	RX	Sent from an iCLASS Hi-O Reader to the control panel indicating the tamper sensor has been triggered.

*Keypad Event is utilized only for iCLASS Readers implementing a keypad.

1.2 Identification Event Data Format

When the iCLASS Universal Core module reads a tag it transmits the card identification using the Identification Event Virtual Device. There are two main types of card data messages:

- HID Credential Data (iCLASS) – Sent MSB first with no start sentinel.
- CSN data (Card Serial Number, MIFARE® or other) – Sent LSB first with no start sentinel.

Hi-O Identification Event messages transmit user data in blocks of 3 bytes per message. Therefore, card data that is not exactly 3 bytes long is split into multiple Identification Event message segments. Zeros are appended after the last bit of card data to fill the 3 byte segment. The maximum number of ID event message segments is 255 (0xFE to 0x00) for a total of 765 bytes of data. (759 bytes of card data + 3 byte Data Format Header + 3 byte Length segment).

The Identification Event requires the first PDO message be a length byte indicating the # of card data bits + 24 for the Data Format Header.

The second message contains a 24 bit Data Format Header. Data format 0 is used for all messages.

The 3rd and following Hi-O messages contain the card data.

To facilitate the reconstruction of data segmented across several messages, each message includes a sequence number.

1.2.1 MIFARE UID Example

Shown is the format of a 4 byte (32 bit) MIFARE UID transmitted using an Identification Event. Table 2 – MIFARE UID Example Data shows 4 bytes of UID data reported by the MIFARE tag.

Table 2 – MIFARE UID Example Data

Byte#	3	2	1	0
MIFARE Standard 4k UID	B2h	6Eh	88h	50h

To match the Wiegand output format with the standard iCLASS Reader, the MIFARE UID data is transmitted as the least significant byte first. The corresponding Hi-O Messages are shown in Table 3 – MIFARE UID Hi-O Messaging Sequence.

Table 3 – MIFARE UID Hi-O Messaging Sequence

	Virtual Device		PDO Payload						
	ID Event	Auth	Seq #	Data					
First Sent PDO (length)	30	63	00	00	00	38h MsgLen byte0	00h MsgLen byte1	00h reserved	
Second PDO (Data Format Header)	30	63	00	00	01	00h Format	00h reserved	00h reserved	
Third PDO (Card Data)	30	63	00	00	02	6Eh byte2	88h byte1	50h byte0	
Last PDO (Card Data+ 0s)	30	63	00	00	03	00h byte5 (padding)	00h byte4 (padding)	B2h byte3	

1.2.2 iCLASS 26 Bit Credential Example

Described is the format used for sending 26 bit iCLASS card data using an Identification Event.

Card Data Recorded

Facility Code = 0x16,
 Credential Number = 0x0016

Standard 26 bit card data is encoded with an additional start sentinel bit, as shown.

SEAAAAAAAABBBBBBBBBBBBO = 1 1 00010110 000000000010110 0

- S = Start Sentinel
- E = Even Parity
- A = Facility Code
- B = Credential Number
- O = Odd Parity

The card data is stripped of the start sentinel and sent out to the Hi-O bus with the following format.
Left Justified, MSB first, zero padding at the end.

The bits to send are: **1000 1011 0000 0000 0000 1011 0000**

(Two 0's are appended to the last nibble to create a full byte.)

Table 4 – iCLASS 26 Bit Credential Example Data

Byte#	0	1	2	3
Card Data	8B _h	00 _h	0B _h	00 _h

Finally, the data sent over the Hi-O network appears as shown in Table 5 – iCLASS 26 Bit Credential Hi-O .

Table 5 – iCLASS 26 Bit Credential Hi-O Messaging Sequence

	Virtual Device ID		PDO Payload						
	ID	Event	Auth		Seq #	Card Data			
First Sent PDO (length)	30	63	00	00	00	32 _h MsgLen byte0	00 _h MsgLen byte1	00 _h reserved	
PDO2 (Data Format Header)	30	63	00	00	01	00 _h FormatHdr	00 _h reserved	00 _h reserved	
PDO3 (Card Data)	30	63	00	00	02	0B _h byte2	00 _h byte1	8B _h byte0	
PDO4 (Card Data)	30	63	00	00	03	00 _h byte5 (padding)	00 _h byte4 (padding)	00 _h byte3 (4 bits + padding)	

1.3 Device Light Control Event Data Format

The iCLASS readers implement a single tri-color light bar as a visual indicator. The light bar has the ability to output Red, Green, Amber and an OFF state.

The Light Control Event defines several light types. Implemented in the iCLASS Hi-O reader are a subset of these light types. The iCLASS Hi-O reader light types are mapped as shown Table 6 – iCLASS Hi-O Reader Light Types.

Table 6 – iCLASS Hi-O Reader Light Types

Light Control Event Types	iCLASS Hi-O Reader LED Color
ACCESS_GRANTED	Green
ACCESS_DENIED	Red
AUX1	Amber

Since the iCLASS reader has a single Tri-Color LED, only one Device Light Control object can be active at a time.

1.4 Device Buzzer Control Event Data Format

The iCLASS Universal reader implements a buzzer as an audible indicator. The Device Buzzer Control object has the ability to control the on/off functions of the buzzer. The buzzer is the COMMON BUZZER device in the device buzzer control command.

1.5 Sabotage Event

An Optical Tamper switch is located on the iCLASS reader main PCB. In the event that switch activity is detected the reader transmits a Sabotage Event over the Hi-O network. See the iCLASS Hi-O Installation Guide, part number 3170-901 for connecting the Tamper/Sabotage Jumper for use with a Hi-O Network.

1.6 Keypad Event

Some models of the iCLASS Reader line (RK40) contain a keypad. The Table 7 – ASCII Table for Keypad Characters shows the ASCII code sent for the corresponding key pressed.

Table 7 – ASCII Table for Keypad Characters

Key	ASCII Code (hex)
0	0x30
1	0x31
2	0x32
3	0x33
4	0x34
5	0x35
6	0x36
7	0x37
8	0x38
9	0x39
*	0x2A
#	0x23
NULL	0x00

Per Hi-O specifications, each ASCII character message is followed by a message containing a null character 0. See Table 8 – Keypad Event Hi-O Messaging Sequence for the Hi-O messaging sequence after pressing the one (1) key.

Table 8 – Keypad Event Hi-O Messaging Sequence

	Virtual Device ID		Auth		PDO Payload			
	Keypad Event				Byte0	Byte1	Byte2	Byte3
1 st PDO (ASCII char 1)	38	63	xx	xx	31	00	00	00
2 nd PDO (Null Char)	38	63	xx	xx	00	00	00	00

1.7 Offline States

If a Hi-O iCLASS reader detects that it is the only unit active on a network, the reader enters the offline state. Default settings for the offline state are shown Table 9 – Offline States but can be customized at the time of installation using Hi-O Manager. Contact your sales representative for access to the Hi-O Manager tool.

Table 9 – Offline States

State	Dir.	Virtual Device	Visual Indication Behavior	Audible Indication Behavior
Unit offline	n/a	n/a	Blink Amber On 500ms, Off 1500ms	Beep Off
Fire Alarm	RX	6240h Fire alarm 6248h Reset fire alarm	Blink Red On 500ms, Off 1500ms	Beep On 500ms, Off 1500ms
Emergency Alarm	RX	6250h Emergency alarm 6258h Reset emergency alarm	Blink Red On 500ms, Off 1500ms	Beep On 500ms, Off 1500ms
Panic Alarm	RX	6260h Panic alarm 6268h Reset panic alarm	Blink Red On 500ms, Off 1500ms	Beep On 500ms, Off 1500ms
System Warning	RX	6220h System warning 6228h Reset system warning	Blink Yellow On 1500ms, Off 1500ms	Beep Off
System Alarm	RX	6230h System alarm 6238h Reset system alarm	Blink Yellow, On 500ms, Off 500m	Beep Off

2 Device Identification

The Hi-O Standard requires certain fields for identification on the Hi-O Bus. The required fields as implemented in the iCLASS Hi-O Reader are shown in Table 10 – Device Identification Values.

Table 10 – Device Identification Values

Name	Length	Value
Vendor ID	4 Bytes	0x06000149
Product Code	4 Bytes	0x31700000
Device Serial Number	4 Bytes	0x00000000 to 0xFFFFFFFF
Firmware Revision	4 Bytes	63519-xx-yy (maps to module code version 6300-519-xx)



Contact

North America
15370 Barranca Parkway Irvine, CA 92618 USA Phone: 800-237-7769 Support: 866-607-7339 Fax: 949-732-2120 Email: tech@hidglobal.com
Europe, Middle East and Africa
Phoenix Road Haverhill, Suffolk CB9 7AE England Phone: +44 (0) 1440 714 850 Support: +44 (0) 1440 711 822 Fax: +44 (0) 1440 714 840 Email: eusupport@hidglobal.com
Asia Pacific
19/F 625 Kings Road North Point, Island East Hong Kong Phone: 852 3160 9800 Support: 852 3160 9833 Fax: 852 3160 4809 Email: asiasupport@hidglobal.com